Spoofing

What it is and what it means to you

Dialog

The following dialog describes the concept of spoofing and what the ramifications are for e-mail users.

Q: I keep receiving e-mails that tell me that I transmitted a virus to another user. Sometimes, they say that I sent a message to an unknown address, but I have no record that I sent any message at all to that user. Why do I get these messages?

A: In a word, the reason for this is called "spoofing", and it's a technique that is commonly used by today's viruses.

Q: What is spoofing?

A: In this case, spoofing is the ability to send an e-mail in such a way that the "From" address (the supposed sender) is a fake, thus hiding the actual sender of the infected message.

Q: How does spoofing work?

A: Let's start at the beginning. A user sits at home reading his e-mail. Hypothetically, we'll call him Bill Evans, who resides in Colorado (but it could be Germany, Australia, Thailand, India, or anywhere else) and has an e-mail address of *bevans@xmail.com*. One of the messages he sees says (for instance) that he sent mail that could not be delivered, with details provided in the attachment. Naturally, he tries to open the attachment, but nothing appears to happen. He puts it down to a system anomaly, but in reality something did happen: the attachment was a virus, and it is now running on his system.

Q: What happens when the virus runs?

A: The first thing the virus does is try to collect as many e-mail addresses as it can from your system. This is called harvesting, and this will be the list of users that it will try to send infected messages to in order to spread even further.

Q: Where do the addresses come from?

A: The virus may scan Bill's address book, but some viruses also can read every Web page that Bill has visited in the past week, month, or even year and extract e-mail addresses that have been provided on them. Or it can open Word files, Excel spreadsheets, or databases and find addresses there. You would be surprised at how many places e-mail addresses are stored. Regardless, these viruses are very successful at harvesting addresses, and the result is usually hundreds or thousands of potential

targets.

Q: After it has these addresses, what happens?

A: The virus then starts to create infected messages that it will transmit to all of those users. This is where spoofing comes in. For each message, instead of using *bevans@xmail.com*, the actual infected user, it will select one of the addresses that it has collected. Let's say that address is *jim.smith@doe.gov* (representing you). It then will send an infected message that appears to be from you (Jim Smith) to all of the other addresses that it has culled. This could number in the thousands.

Q: But those messages are *from* me, not *to* me. How does that cause the messages that I get?

A: The messages you receive are responses to the infected transmissions. Today, most major e-mail providers, whether they are ISPs (like AOL, Yahoo, or Hotmail) and businesses (such as DOE) automatically check incoming messages for viruses or other undesirable mail. For our example, let's say that one of the addresses that was harvested was *john.doe@abccorp.com*. Thus, one of the virus e-mails would be from you to *john.doe@abccorp.com*. When *abccorp.com* receives that message, it could result in the generation of three types of messages:

- Some of the harvested addresses turn out to be invalid, perhaps because the virus incorrectly picked up an address, an invalid address was posted on a Web page, or the address is outdated and the user is no longer there. So let's say that John Doe no longer works at ABC Corp. The post office at *abccorp.com* will recognize that this is an invalid address and attempt to send a message back to the original "sender" to let them know (just as the U.S. Post Office returns your "undeliverable" mail back to you). Unfortunately, because of spoofing, *abccorp.com* thinks that the sender was *jim.smith@doe.gov* (you). When you receive this "bounce-back" message, you of course cannot find any record of having sent *john.doe@abccorp.com* a message, which causes some confusion. Examples of this type of message may look as follows:

```
From: postmaster@abccomp.com
Your message
To: John.Doe@abccorp.com
Subject: RE:
Sent: Mon, 9 Aug 2004 19:43:56 -0400
did not reach the following recipient(s):
john.doe@abccorp.com on Mon, 9 Aug 2004 18:44:59 -0400
The recipient name is not recognized
```

- ---------- OR ----------

```
From: postmaster@abccomp.com
To: Smith, Jim
Subject: Delivery Status Notification (Failure)
```

> Sent: Friday, June 04, 2004 2:02 AM
> This is an automatically generated Delivery Status Notification. Delivery to the following recipients failed:
> John.doe@abccomp.com

- Some post offices automatically reject messages with certain characteristics, such as those that have attachments. This is called a policy block. As with the undeliverable notice, the post office may look at the infected message, see that it has an attachment, and reject it, again sending a notification message back to the "sender" (you). Once again, you are confused. An examples of this type of message may look as follows:

> From: antigen@abccomp.com
> Antigen for Exchange found mail0.pif matching FILE FILTER= *.pif file filter. The file was removed. The message, "Re: Mail", was sent from jim.smith@doe.gov."

- The final, and most common, message is the virus bounce-back. Because the message does contain an infected attachment, most post offices will perform a virus scan, detect the infection, and block the message. Many post offices also will generate a notification to the "sender", once again alerting the wrong user. This time, the notification causes more than confusion; it causes concern. Messages of this type may look as follows:

> From: webshield@abccomp.com
> VIRUS INFECTION ALERT
> The WebShield® e500 Appliance discovered the W32/Bagle.a virus in this file. The file was not cleaned and has been removed. See your system administrator for further information.

- ---------- OR ----------

> From: postmaster@abccomp.com
> A message sent by you was blocked by content protection for Novell GroupWise.
> The message was blocked for the following reason(s):
> Virus infection

Q: But some of the message I received look like they came from other DOE users. Should I be more concerned?

A: Given that the virus found your address on the infected system, we shouldn't be too surprised that it managed to find other DOE addresses as well. Therefore, some of the generated mail will have DOE addresses for both the sender and recipient. This may cause some notifications to look like they are internal, but in actuality they are not. These messages should be treated no differently than any other false notifications.

Q: I understand that spoofing viruses have been around for a few years. Why are we seeing so many more false notifications today?

A: It has to do with volume. Today's viruses seem to be infecting more users, staying active for longer periods of time (often because the users don't know they are infected,

because they aren't receiving the virus alerts that are going to the spoofed senders), and generating more messages than ever. As an example, some monitoring sites have reported that they are stopping more infected messages *per month* in 2004 then they did in *all* of 2003. This means that it is much more likely that your address will be used in a spoof and that you will receive a false bounce-back.

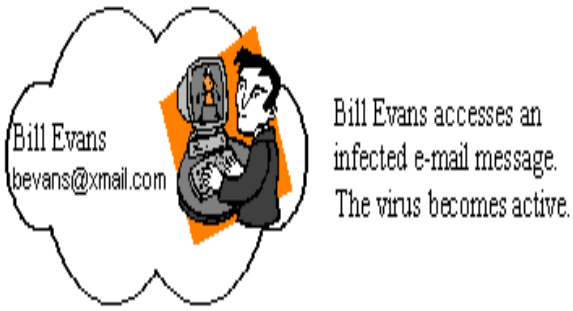
Q: So what should I do?

A: In nearly all cases, the recipients of the bounce-back are NOT infected users, especially if their systems access a protected post office, which most do. At DOE, we have numerous layers of protection, so it is highly unlikely that your system is infected. We recommend that you ignore and delete these notifications. Unfortunately, there is no way to trace back to the actual infected user, so there is no beneficial action that can be taken. And Bill Evans will continue to use his system, unaware that it is generating thousands of infected e-mails every day.

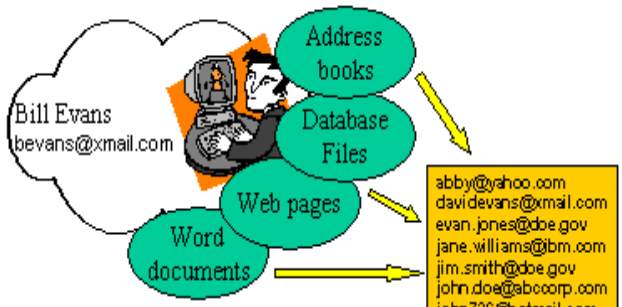
Summary

In summary, this is how spoofing works:

1. A system gets infected when a user accesses an infected e-mail.

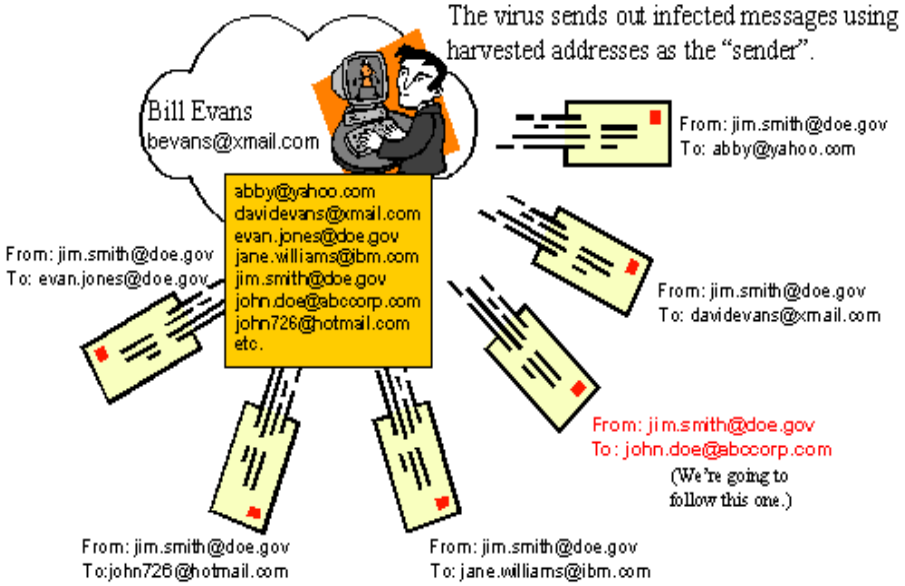


2. The virus harvests e-mail addresses from the infected system.

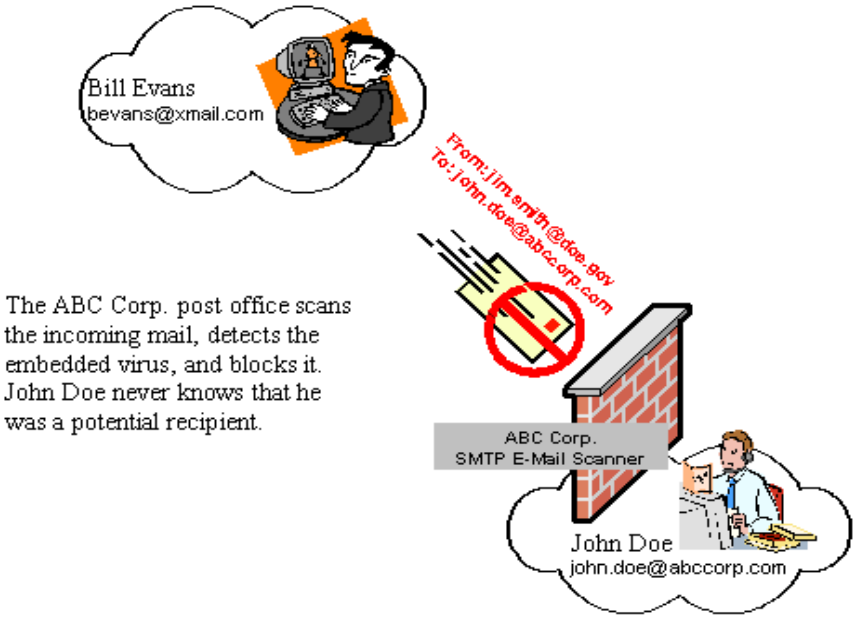


The virus harvests a list of e-mail addresses from address books, documents and databases, Web pages, and other sources.

3. The virus sends out infected messages using one of the addresses as the "sender".



4. Receiving sites block the incoming messages.



5. In many cases, they send notifications back to the "sender", who is not the actual infected user.